80

# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/775,205 | 02/01/2001 | Alan Boate | RIDM.P-002 | 7111 |

32692 7590 08/11/2005

3M INNOVATIVE PROPERTIES COMPANY
PO BOX 33427
ST. PAUL, MN 55133-3427

| EXAMINER |
|---|
| SHIFERAW, ELENI A |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

DATE MAILED: 08/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>09/775,205 | **Applicant(s)**<br>BOATE ET AL. | |
| | **Examiner**<br>Eleni A. Shiferaw | **Art Unit**<br>2136 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *17 May 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

10

## Detail Action

### *Response to Amendment*

1. Applicant's arguments/amendments with respect to claims 1-22, filed on May 17, 2005 have been fully considered but they are not persuasive. The examiner would like to point out that this action is made final (MPEP 706.07a).

### *Response to Arguments*

2. Applicant argues that:

a. Independent claims 1, 9, and 17 are not taught by Martizen, Bolle and Etzel alone or in combination to include *"a personal digital identifier device that includes a biometric component, and a processor that evaluates whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component*", (page 2 par. 3-page 3 par. 1).

b. The references, whether alone or in combination, fail to support *"generation of a public and a private key within a portable personal identification device"*, (page 3 par. 3-page 4 par. 2), on all independent claims.

c. Neither of the references teaches limitation on claim 17 wherein *"permitting authenticated user to access said computer network through the workstation"* (page 4 par. 4).

d. Etzel fails to disclose wherein *"a personal digital identifier device wherein all data held in said secure storage is by itself non-identifiable of said user"*, (page 4 par. 5), on dependent claims 4 and 14.

e. Martizen, on claims 15 and 20 of the dependent claims, fails to teach wherein *"a security system wherein said network storage includes data identifiable of said user for display on a screen of said workstation when said user's personal identification device is located within said envelope"*, (page 5 par. 2-3).

f. Rydbeck, on claim 22, fails to suggest wherein *"a policy manager component may direct that the screen of said workstation be blanked out when a new personal digital identifier device moves to a location within said envelope until such time as the user registered to said personal digital identifier device is biometrically identified"*, (page 5 par. 4-page 6 par. 3).

g. Dependent claims 2-3, 5-8, 10-11, 13, 19, and 21 are allowable based upon their dependency on allowable claims 1, 9, and 17.

However, Examiner disagrees with applicant.

Regarding argument (a), Argument is not persuasive. Bolle teaches generating biometric template on a wireless device and storing the generated biometric template only locally in the wireless device to reduce the chances an intruder accessing biometric data (col. 3 lines 36-44), because the biometric data generated and stored in database accessible over a network is susceptible to attacks from intruders (Abstract, and col. 3 lines 20-21). In short, biometric template is not generated or stored outside the wireless device.

Authentication is performed by comparing the originally stored biometric template with the measured biometric/provided/inputed by the user in the wireless device (col. 3 lines 46-49 and fig. 8 element 804).

Regarding argument (b), Argument is not persuasive. Etzel discloses generating a unique device encryption key and related public key that is never disclosed to another device entity ("externally unknown") and the private and public key in local memory (col. 1 lines 53-59), and examiner suggested that it would be obvious to combine Etzel within Martizen and Bolle because it would provide a strong way of controlling and maintaining the secrecy of the intelligence used by computers to communicate with one another as cited in the office action page 6.

Regarding argument (c), Examiner disagrees with applicant. Martizen teaches authenticated user and access to the network is granted (fig. 17 element 13).

Regarding argument (d), Applicant is not persuasive. Etzel teaches data stored in the storage by itself is not identifiable by user (see, col. 1 lines 53-59).

Regarding argument (e), Applicant is not persuasive. Martizen teaches locating the wireless device of a user within the envelope and identifying and sending identified data to user to be displayed (see, fig. 17 element 13, page 15 par. 0202-0203, and page 16 par. 0210).

Regarding argument (f), examiner disagrees with applicant. Rydbeck discloses performing no action when unidentified wireless device is detected (Rydbeck col. 6 lines 41-65).

Regarding argument (g), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a) - (f), the dependent claims stand rejected.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts that the system of the prior art, references do teach or suggest the subject matter as recited in independent claims 1, 9, and 17. Dependent claims 2-3, 5-8, 10-11, 13, 19, and 21 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action dated May 17, 2005. Accordingly, rejections for claims 1-22 are respectfully maintained.

3. Claims 1-22 are pending.

**Rejections**

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maritzen et al. (Maritzen, U.S. Pub. No. US 2002/0073042 A1) in view of Bolle et al. (Bolle, Patent No.: US 6,819,219 B1) and Etzel et al. (Etzel, Patent No.: US 6,577,734 B1).

As per claim 1, a personal digital identifier device (Page 1-2 par. 0032; transaction device which has a unique identifier comprising privacy card and digital wallet) for controlling access to a computer network, said network comprising a plurality of workstations each having a base unit associated therewith, said base unit being configured for wireless communications with said personal digital identifier device (Page 19 par. 0250; wireless base station), and said network further comprising a central server utilizing a security manager component and network storage (Page 5 par. 0063; TPCH embodied as a secure server for authentication), said security manager component associated with a private key and a corresponding public key and a public key corresponding to a private key held by said personal digital identifier device (Page 2 par. 0039, page 11 par. 0157; PKI and private key respectively), said personal digital identifier device being lightweight, configured for wearing and/or carrying by a user registered thereto (Page 6 par. 0082; easy sized carrying privacy card) and comprising:

(a) a wireless communications component comprising a transceiver for communicating with said base unit; (Martizen Fig. 14 and page 17 par. 0023; digital wallet in communication with a base unit)

(b) a biometric acquisition component for obtaining a user's input biometric; (Page 2 par. 0038, page 19 par. 0251, page 20 par. 0259, fig. 7c, and 21; digital wallet stores users biometric information to authenticate a user wirelessly)

(c) a processor configured for communicating with said transceiver and said biometric component and operable for (Page 14 par. [0184-0185], page 8 par. 0103):

(i) evaluating whether the a template stored corresponds to a master template stored on biometric digital representation and generating a matching signal when such a correspondence is determined; (Page 2 par. [0038-0043], page 8 par. 0103]; evaluating whether the given template corresponds to the master template stored on the digital wallet);

(iii) producing a digital signature using said private key; (Page 11-12 par. [0157-0167]) and,

(iv) verifying, using said public key for said private key associated with said security manager component, that the source of an encrypted message ostensibly received from said security manager is said security manager component (Page 2 par. 0039);

(e) a power source; (Page 6 par. 0079; temporary battery, page 7 par. 0091, page 8 par. 0109, and fig. 14) and,

(f) a housing, (Fig. 8)

said personal digital identifier device being configured for, a digitally signed challenge response message following said generating of said matching signal in response to a challenge message received from said security manager component and for transmitting said response message (Page 5 par. [0066-0068]),

Maritzen does not explicitly teach:

(b) personal digital identifier producing a digital representation thereof;

(d) secure storage containing said master template of a user's biometric associated with said security manager component; and

said personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric;

However Bolle discloses generating a digital representation (master biometric template) (Bolle Col. 4 lines 53-64, and col. 5 lines 35-39);

master biometric template generated locally on the wireless device is stored securely on the wireless device locally and master biometric data is never transmitted (Bolle Col. 7 lines 59-col. 8 lines 2);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Bolle within the system of Maritzen because it would prevent an intruder from accessing biometric data by storing the biometric template locally and never transmit the template from the wireless device (Bolle Col. 7 lines 63-65);

Maritzen and Bolle do not explicitly teach:

(c) (ii) generating said private key held by said personal digital identifier device and said public key corresponding thereto and outputting said generated public key for transmission by said transceiver;

(d) secure storage said generated private key and said public key for said private key;

(f) personal digital identifier device being configured for producing, using said generated private key;

However Etzel discloses generating a unique device encryption key and related public key that is never disclosed externally to another device or entity ("externally unknown") and stores the private and public key in local memory (Etzel Col. 1 lines 53-59).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Etzel within the combination system of Martizen and Bolle because it would provide a strong way of controlling and maintaining the secrecy of the intelligence used by computers to communicate with one other (Etzel col. 1 lines 43-57);

As to claim 9, it has similar limitations as claim 1; therefore, it is being rejected under the same rationale over Maritzen, Bolle and Etzel. In addition, Martizen teaches:

B. a base unit associated with said workstation and configured for initiating and maintaining wireless communications with said personal digital identifier device, said communications extending over an area defined by an envelope associated with said workstation (Martizen page 15 par. [0202-0203]; digital wallet and personal computer in wireless communication in the same region or LAN); and

C. a server having access to network storage to authenticate a user that reads on a central server having access to network storage and utilizing said security manager component and said personal digital identifier device for authenticating said user (Martizen Fig. 17 and page 2 par. 0039; digital wallet and TPCH authenticating a user).

As to claim 17, it has similar limitations as claim 9; therefore, it is being rejected under the same rationale over Maritzen, Bolle and Etzel. In addition, Martizen teaches:

(a) on registration of a portable personal digital identifier device to a user, within said portable personal digital identifier device: receiving an input biometric of said user (Maritzen page 11 par. 0143);

(b) transmitting a first signal from a base unit associated with one said workstation to said personal digital identifier device and automatically transmitting from said personal digital identifier device a response signal establishing communications between said base unit and said personal digital identifier device in response to said first signal when said personal digital identifier device is within said envelope (Maritzen page 15 par. 0202 and 0206; wireless digital wallet in signal communication with personal computer wirelessly);

(c) receiving at said personal digital identifier device a digitally signed challenge message ostensibly from said network security manager component and verifying within said personal digital identifier device the origin of said challenge using said public key for said private key associated with said security manager component (Maritzen Page 2 par. 0039 and Bolle Fig. 6 No. 1 and 4);

(g) permitting said authenticated user to access said computer network through said workstation (Maritzen Fig. 17 No. 13).

As per claims 2 & 10 the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches a personal digital identifier device (system) wherein said biometric component includes a transducer (Page 3 par. 0043, page 6 [0080-0085]; fingerprint recognition built in the card).

As per claim 3, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches personal digital identifier device wherein a response signal is automatically transmitted from said transceiver in response to a signal received by said transceiver from one said base unit (Page 7 par. 0091, page 17 par. 0221, page 20 par. 0256, fig. 21).

As per claims 4 & 14, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Etzel teaches a personal digital identifier device wherein all data held in said secure storage is by itself non-identifiable of said user (Etzel Col. 1 lines 53-59). The rational for combining are the same as claim 1 above.

As per claim 5, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches a personal digital identifier device wherein said transducer comprises a solid state fingerprint sensor (Maritzen Page 3 par. 0043, page 6 par. [0080-0085]).

As per claim 6, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches a personal digital identifier device wherein said transceiver transmits and receives optical signals (Maritzen Page 8 par. 0111).

As per claim 7, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches a personal digital identifier device wherein said transceiver transmits and receives radio frequency signals (Maritzen Page 6 par. 0079-0080).

As per claim 8, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches a personal digital identifier device in combination with a device holder wherein said device holder is configured to co-operate with said housing of said personal digital identifier device such that said personal digital identifier device is held by said holder device when it is appropriately positioned relative to said holder device, said device holder comprising a communications connector for communicatively coupling said personal digital identifier device directly to one said workstation when said personal digital identifier device is held by said device holder (Maritzen Fig. 8, 9a, 9b; digital wallet and privacy card, page 1-2 par. 0032, and 0038).

As per claim 11, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches a security system wherein said workstation is a personal computer (Martizen page 15 par. 0202).

As per claim 12, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches a security system wherein said base unit regularly transmits a first signal to said personal digital identifier device and said personal digital identifier device automatically transmits a response signal in response (Maritzen page 15 par. [0202-0206] and fig. 17; signal transmissions to conduct shopping activity in using wireless digital wallet).

As per claim 13, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches a security system comprising a plurality of said personal digital identifier devices, a plurality of workstations and a plurality of base units wherein a base unit is associated with each said workstation, each said base unit transmitting a polling signal to each said personal digital identifier device within said base unit's associated envelope following said base units receipt of said response signal from each said personal digital identifier device. (Page 15 par. 0202 and page 11 par. 0152; wireless digital wallets are in communication with personal computer in the same region or LAN).

As per claim 15, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches a security system wherein said network storage includes data identifiable of said user for display on a screen of said workstation when said user's personal identification device is located within said envelope (Maritzen Fig. 17 No. 13 and page 16 par. 0210; secure electronic content distribution is transmitted to the user for display).

As per claims 16 and 18, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. A security system wherein said envelope has a shape and area which are configured to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation. (It is inherent to have an envelope with shape and area to encompass locations proximate, the examiner points out this reference: Gainsboro et al. Pub. No.: US 2001/0036821 A1 Fig. 4, Page 6 par. 0058).

As per claim 19 the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. Further comprising, following said base unit's receipt of said response signal from said personal digital identifier device, transmitting from said base unit a polling signal to said personal digital identifier device for determining whether said personal digital identifier device remains located within said base unit's associated envelope (It is well known to send a polling signal to the wireless device because it would determine whether the wireless device is within the envelope region; the examiner points out: Reed, Patent No.: US 6,754,504 B1 Col. 7 lines 13-36).

As per claim 20, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches further comprising displaying on a screen of said workstation data identifying said user when said user is identified. (Maritzen Fig. 17 No. 13 and col. 15 par. [0202-0203]; user is authenticated and identified and content is provided to display on the users computer).

As per claim 21, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above. In addition Maritzen teaches further comprising initially registering said user by a registrar in the presence of a guarantor, said registrar and guarantor each being a registered user of the computer network and said registrar having access to the computer network and verified by said security manager component to have registration privileges, and requiring: that said guarantor provide to said security manager component a biometrically digitally signed message to authenticate said guarantor and that each of said registrar, guarantor and user remain within said envelope during said registering of said user (Maritzen page 2 par. 0039, and fig. 17 No. 13; user biometrics is registered and digital wallet is used to authenticate the user and content is provided from the network server to the user's PC)

6. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Maritzen et al. (Maritzen, U.S. Pub. No. US 2002/0073042 A1) in view of Bolle et al. (Bolle, Patent No.: US 6,819,219 B1) and Etzel et al. (Etzel, Patent No.: US 6,577,734 B1) and in further view of Rydbeck et al. (Rydbeck, Patent No.: US 6,195,564 B1).

As per claim 22, the combination of Maritzen, Bolle and Etzel teach the subject matter as claimed above.

Maritzen, Bolle and Etzel do not explicitly teach whereby a policy manager component may direct that the screen of said workstation be blanked out when a new personal digital identifier device moves to a location within said envelope until such time as the user registered to said personal digital identifier device is biometrically identified.

However Rydbeck discloses a communication device and a wireless device determining whether an electronic message is to be transferred by checking the elapsed time and sending a paging signal to the wireless device and if the wireless device is not responding to the signal, the wireless device returns to the standby state or not activated to transfer message (Rydbeck col. 6 lines 41-65).

Therefore it would have been obvious to one having ordinary skill in the art at time the invention was made to modify the teachings of Rydbeck within the combination system of Maritzen, Bolle and Etzel because it would allow to control access. The base unit checks the if the personal digital identifier (pdi) device is responding, if the pdi is not responding the base unit transmits data to the network server and the network server would blank user screen (access denied signal) until user is biometrically identified.

## *Conclusion*

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw

August 2, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100